About SISS Data Services

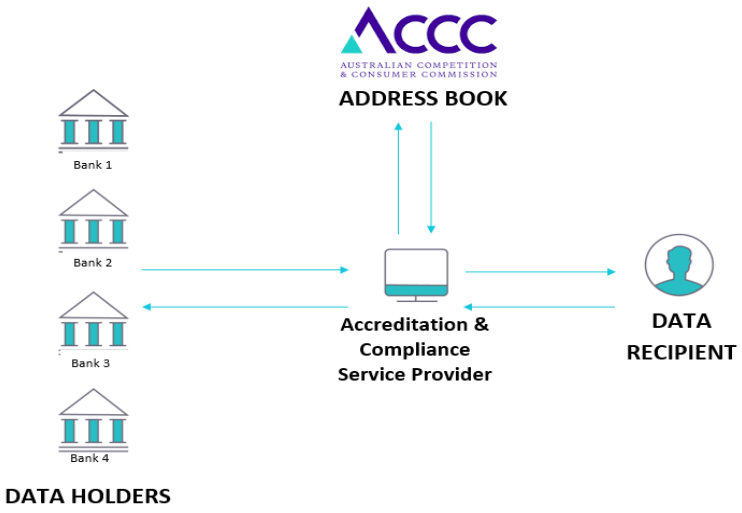
SISS Data Services provides an Open Banking Platform supporting Financial Institutions (Data Holders) and Fintech's (data Recipients). For over 7 years SISS has provided consent driven, API access to Financial Institutions, including the 4 major banks, for 3rd party (Data Recipients). SISS is Australia's largest Open Banking API provider supplying bank data feed for over 150,000 Australians.

The Role SISS performs in the Open Banking Environment

Open Banking Platform for **Data Recipients** to access multiple **Data Holders** via a Rest API

Open Banking Platform for **Data Holders** to share consumer data with **Accredited Data Recipients**

Accreditation tool (software) for **Data Recipients** to be accredited under the CDR



Please note our section numbering aligns with the section numbering in the Consumer Data Right Rules Framework September 2018

2. Sharing Data with 3rd Parties

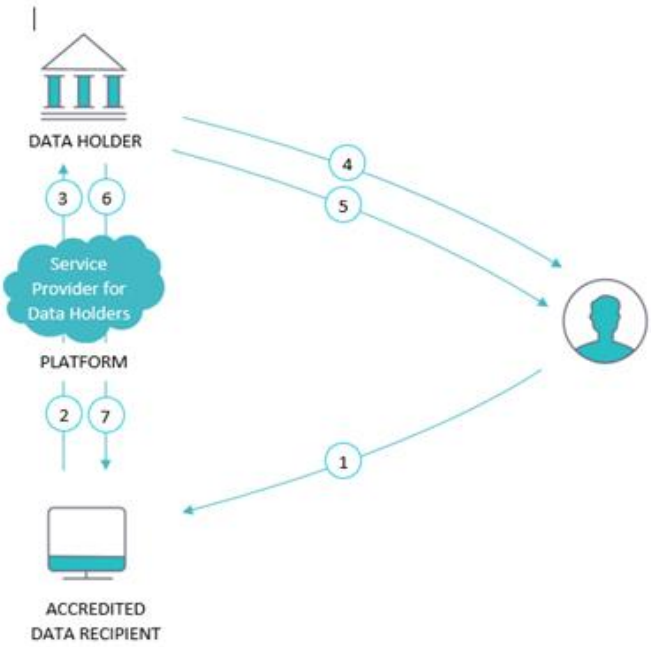
Summary

1. SISS agrees with sharing via an API
2. Propose that it is acknowledged that Data Holders may engage a service provider to deliver there in a CDR compliant format, and these service providers must also comply with the CDR and ACCC rules.
3. SISS agrees that a fee should not be charged for access to the data
4. SISS agrees that derived data should not be included in the fee free status.

2.2 Sharing via an API

SISS agrees that the most efficient method of data sharing is via an API, our experience is that the technical skills and cost to implement vary from Data Holder to Data Holder.

The CDR needs clearly recognise the role that service providers (Platforms) can play in providing Data Holders (e.g. Banks) with the infrastructure they need to make data available via an Open Banking API.



1. The consumer consents to the accredited data recipient obtaining their data
2. The accredited data recipient seeks access to the consumers data and their identity and accreditation status is by via an approved **Platform**
3. The **Platform** connects to the Data Holder with the request from the accredited data recipient
4. The Data Holder authenticates the identity of the consumer
5. The consumer authorises the data holder to disclose their data to the
6. The data provides the consumer and consumer data to the Platform
7. The Platform shares the consumers data with the accredited data recipient

2.3 Sharing Must not Attract a Fee

In our experience working with software companies wanting to consume bank data the cost of the data from Data holders has prohibited innovation and is a barrier for new entrants. Historically, access to bank data has attracted a "per line item" fee which can disadvantage high transaction accounts. By not charging a fee for data, we believe this will drive innovation and attract new participants.

3. CDR Data – Who May Take Advantage of the CDR

Summary

1. SISS agrees that with the consumer definition being extended to Individuals, Businesses and sub sets such as trusts
2. SISS agrees that former customers do not need to be included in the first version of the CDR rules
3. SISS ***does not agree*** that offline customers be excluded.

3.2 Offline Customers

The current method of authorising data from Data Holders requires a paper based from to be completed and submitted to the bank. Where a consumer is not an online customer, or due to age or disability cannot access services online, they will be disadvantaged under this proposal.

We recommend that Offline customers be able to submit a paper-based authorisation where they fall in one of 3 categories:

1. Not an Online Customer
2. Due to Age or Disability are unable to access online services
3. Special consideration e.g. Medical or other

A standard paper-based form that complies with the ACCC frame work can be created by the ACCC and used by all data holders.

For a Customer who is not digital but needs to grant access to their accountant, guardian, legal representative they will have no mechanism under CDR. Note: This offline model exists today and is used by many providers such as MYOB/BankLink, Xero and SISS. Excluding the offline model would be a step backwards.

5. Data Sets- What Data is within Scope

Summary

1. SISS agrees with the proposal under Section 5.2
    a. Metadata we think should be available
        i. Merchant details – Address, Location, Latitude, Longitude,
        ii. Tax details
        iii. What was purchased.
2. SISS recommends that the UK approach to Credit Card Numbers (PAN) be followed to avoid PCIDSS issues which might impact consumers if the accredited data recipient is breached.
3. If not already provided for, SISS recommends that a balance only enquiry is included in the data set
4. Data holder should be required to map transactions to the global standard messaging framework ISO 20022, as per the ideal UK model.

5.3.1 Customer Data

For a standard read of an account entity, Credit Card Numbers (PAN) should *not* be transmitted within the CDR, as this adds a level of complexity and risk by bringing into scope the Payment Cards Industry Data Security Standards (PCIDSS) for all entities who access this data.

As per the UK OpenBanking spec (v3.0):

"If the ReadPAN permission is granted by the Consumer - the data holder may choose to populate the OBReadAccount2/Data/Account/Account/Identification with the unmasked PAN (if the PAN is being populated in the response)."

6. Accreditation

Summary

- Accreditation needs to be an annual process.
- Data Recipients to perform regular security scans and report monthly CDR participants.
- Product Register for Accreditation solutions that assist Data Holders and Data Recipients comply with CDR accreditation.
- The accreditation process needs to cover 6 main areas:
    1. Disclose
    2. Data Breach Reporting
    3. Risk Management
    4. Consumer Compliant Register
    5. Security Monitoring & Reporting
    6. Insurance Register
- To manage and reduce risk, all participants (data holders, ACCC and data recipients) need access to the compliance process.
- Minimum level of cover and coverage needs to be agreed to ensure all participants are covered.
- API connectivity to ACCC Accreditation Lodgement

Background

The accreditation process for Data Recipients is a critical process in establishing a secure, robust and innovative Open Banking environment. If the bar for accreditation is set *too low*, this will put the Consumer data at risk. We could have a situation where the data held and transferred by a Data Holder is of the highest security standard to a Data Recipients' environment which is not adequately secure. If a data breach occurs this put the Consumer, Data Holder and ACCC at risk.

Conversely, if the accreditation bar is set *too high*, for example requiring a start-up FinTech to attain ISO 27001, innovation will be stifled and the take up of data via Open Banking will be limited and Consumers will not see the benefits of Open Banking.

An inherent risk for the accreditation system is the lack on independently verified responses from Data Recipients. Put another way, often responses from Data Recipients to software and data security are *aspirational* rather than factual, giving all CDR participants a false sense of security. This risk is currently overcome by Qualified Security Assessor (QSA) auditing the Data Recipients systems and/or responses.

For example, a Data Recipient may be asked "*Do you perform daily Vulnerability Scanning?"* as a means to ensure a minimal level of system security. The answer may be Yes, but how does the Consumer, ACCC or Data holder know if a Vulnerability scan has been performed? There is a role for independently verified processes.

The cost of QSA in the accreditation would be a barrier to entry, however there are key processes and information that can be verified.

Our approach to accreditation under the CDR has been to understand the security issues and concerns of the consumers, Data Holders (Banks) and Data Recipients (Fintech) and balance those against the needs of the Consumer and the innovation of Data Recipients.

Accreditation needs to be an annual process.

Due to the complexity and changing nature of Data Recipients, the accreditation process for Data Recipients needs to be an annual process to ensure the best practices for data security are meeting both the initial and ongoing accreditation obligations.

Data Recipients innovate and develop at a fast pace their service offerings, methods of data use, storage and transmissions often change. As their data use, storage and transmission will changes and therefore their profile needs to be resubmitted no less than once in a 12-month period.

Accreditation needs to be Frictionless

To balance their accreditation obligations, a frictionless approach to accreditation needs to be implemented. Data Recipients are often small businesses with limited time and resources and as such cannot spend excessive time complying accreditation requirements. This approach needs to include:

1. Rollover of accreditation answers
2. Automated Security Scanning

Data Recipients to perform daily security scans and report monthly.

Data Recipients need to protect the Consumers data. To do this they must regularly monitor their systems and make the results of the monitoring available to both Data Holders and the ACCC.

The security monitor needs to include:

1. Internal Vulnerability Scan
2. External Vulnerability scan
3. Web Application Scan

Use of Scanning over Penetration Testing

Reviewing the history of Data Breaches from the last year[1], there are several themes that are consistent.

- Approx. 75% of attacks originate externally
- Over 50% of all attacks are against small businesses.
- Almost half utilised hacking (getting in via weaknesses in the systems)

External attackers (hackers) are looking for systems which are either not up to date with the most recent patches, have a fault with how they have been configured or have a weakness that no one knows about. They will exploit any of these weaknesses to gain access and execute their desired outcome. A recent example of this is a takeover of routers in Brazil, even though patches have been available for more than 6 months.

Whilst there are a lot of areas that could be focused on, removing the “known” weaknesses from the environments shifts the bar in a positive way for data recipients. These "known” weaknesses will be well covered by Vulnerability Scanning and Web Application Scanning.

Vulnerability Scanning works by analysing systems against the known, published vulnerabilities from the Common Vulnerabilities and Exposure Database (CVE) (which is maintained at https://cve.mitre.org/). Vulnerability Scanning products such as Qualys, Tenable.io or Rapid7, encode these rules in their products and look for attached systems missing the fixes. IT staff then need to work through the list of gaps, correcting the systems, so that they can be scanned again to verify the fixes are in place.

Internal Scanning will only highlight what is missing within systems, while external scanning will highlight if there are any items missing when viewed externally.

[1] Verizon 2018 Data Breach Investigations Report - https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Web Application scanning sits a level above Vulnerability Scanning. This process scans the web applications deployed on a system for vulnerabilities in how they have been coded. Web Application scanners are taking the vulnerabilities from groups such as OWASP (OWASP Top 10), encodes the rules, and then the scanner pretends to be a user visiting all parts of a site. Whilst doing this, it evaluates the coding against best practices. Again, any issues are highlighted, and developers work through the required fixes.

Additional scanning capabilities, such as monitoring the configurations of systems for compliance against best practices, should also be considered.

As these are all automated capabilities, they are often a very cost-effective way of immediately lifting the security profile of a company. Using the 80/20 rule as an analogy, they will deliver 80% of the benefit for 20% of the cost. However, they will not catch everything, so they are generally considered as one component of a good security program. They can also only test what they have been exposed to, so if some systems are excluded, then these tools will not report on them.

A penetration test involves a white hat hacker being paid to evaluate a company's systems to identify gaps. They will do this using many tools, including automated ones. They may also engage in things like social engineering to verify if documented procedures are followed. During this process, they will use their experience to identify areas that could be attacked and may even demonstrate how. It is a very in-depth process, but they may miss some systems if they are not made aware of them. They will produce a report highlighting what needs to be worked on. A penetration test is quite an expensive exercise, as it requires a person or team of people use an intuitive process to identify areas of weakness.

Using the 80/20 analogy, for 80% of the cost, you may identify the remaining 20% of the weaknesses. Unfortunately, even if you exercised both programs, you will not catch 100% of all weaknesses.

In a comprehensive security program (such as PCI DSS or ISO 27001), all of the above measures are required, along with many other requirements for companies to meet. Vulnerability scanning should be frequent (monthly or more frequent) and a penetration test needs to be done on any major functionality change to a system.

For small to medium data recipients, the cost of a single penetration test will be a sizable portion of their budget for the year. If they are working in an agile fashion, they may be releasing multiple major functionality changes every couple of weeks. A penetration test after all of these will be very expensive and time consuming. This may lead to companies crippling their innovation to ensure they do not trigger frequent penetration tests.

For these same data recipients, the introduction of automated vulnerability scanning will generally not be a large cost, and these scans be run hourly with no additional charges. There is a requirement of time for someone to monitor (there is no dedicated resource), get issues corrected and report on a regular basis the status of the systems. While nobody likes doing this, it can be accommodated reasonably easily.

For data holders, who are generally large companies, this is the norm of doing business. These security programs are intrinsic to their business and they can support internal teams to run the programs. The data holders are also not generally revamping their systems on a frequent basis. Specifically, they would not be introducing major functionality on a weekly or monthly basis which would trigger a penetration test.

Even with all the systems, policies and procedures in place, an attack may still succeed if it is using an a previously unreported attack vector.

Product Register for technology solutions that streamline and reduce costs of Accreditation.

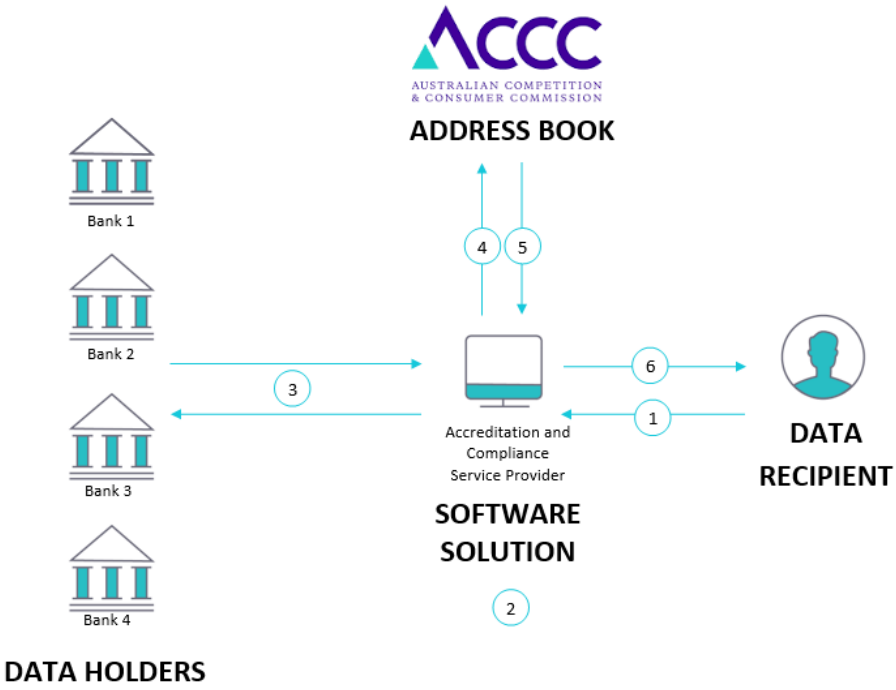
Opening Banking accreditation solutions already exist and need to be acknowledged

Software solutions that assist Data Recipients to comply with their Open Bank obligations need to be acknowledged as a participant in the regulatory framework.

SISS recommends a register like that used for the Standard Business Reporting (SBR) or a similar process, be established to maintain a register of software vendors to register and build to the ACCC compliance lodgement service.

Functionality of the products registered are listed in an online portal.

a. Service can register with the ACCC on behalf of a recipient.
b. Registered Recipient can link Service to the ACCC
c. Centralised point for banks, ACCC & consumers to have visibility of
    a. Status of applications
    b. Risk register & actions to mitigate the risks
    c. Library of vulnerability reports
    d. Reporting and monitoring of data breaches
    e. Repository of a software solutions legal information, key people, contact points, data usage, data policies, technology & security policies, level of insurance and dispute resolution processes.



1. **Data Recipients** registers with Online Portal and completes accreditation requirements and submits requests to data holders
2. **Accreditation Service Provider** performers security scan and makes result available to Data Holders.
3. **Data Holder** reviews application for access to data and approves or rejects with reason
4. Via an API call application is submitted to the **ACCC Address Book**
5. **ACCC Address Book** updates status updated via API
6. **Data Recipient** can access accreditation status via Accreditation Service Provider

The Accreditation Process

Below SISS has noted the evidence or processes the data recipient would need to submit under ***6.2.1 Criteria for general level accreditation*** of the Consumer Data Right Rules Framework September 2018.

The table below aims to address the inherent and significant risk of an accreditation system, which is verifying the responses from a Data Recipient in a cost effective and frictionless way.

No.	ACCC Requirement	Evidence
1	whether the applicant (or its directors) has been charged with or convicted of a serious criminal offence, or an offence of dishonesty, against a law of the Commonwealth or of a State or Territory	• Applicant(s) and Director(s) to provide Police Check.
2.	whether the applicant (or its directors) has been found to have contravened, or civil proceedings have been commenced against the applicant alleging contravention of, a law relevant to the management of CDR data including the Competition and Consumer Act 2010 (Cth) (CCA) (including the Australian Consumer Law), the Australian Securities and Investment Commission Act 2001 (Cth) (ASIC Act) and the Privacy Act 1998 (Cth) (Privacy Act)	• Applicant(s) and Director(s) to provide Police Check.
3.	whether any directors of the applicant have been disqualified from managing corporations	• ASIC disqualified directors report
•	whether the applicant or its directors has a history of bankruptcy or insolvency	• NPII bankruptcy report (National Personal Insolvency Index)
•	any other relevant matter	• Anti-Money Laundering (AML) and Counter Terrorism Financing (AML/CTF) • Related parties disclose • Sensitive Shareholders
•	a business plan, including a detailed description of the services the applicant intends to provide to consumers using CDR data and examples of the relevant consent screens	• Company details (name, ABN Registered Address) • Director(s) Details • Ownership Structure (e.g. Sole trade or Public Company) • List of product and/or service names • Stage of Product lifecycle • Data Use • Data destruction process • Data Types • List personal identifiable information captured. • Location of data storage • Third Parties that connect to your platform

		• Consent flow – screenshots or other presentation mechanism • List current Certification and accreditation
•	evidence of the applicant's internal control mechanisms, including: • if applicable, the details of outsourced activities relating to CDR data (see section 6.8 below) and of the policies and procedures in place to manage those arrangements • information about business continuity arrangements, including clear identification of critical operations, effective contingency plans, and procedures for testing and reviewing of the adequacy of such plans	• Outsourcing arrangements • Provide or describe Information Security Policies Specifically a. Data Classification Policy b. Data Destruction Policy c. BCP Policy d. DR Policy e. Risk Management Policy
•	evidence of the applicant's risk management processes, including: • effective procedures to identify, manage and monitor any risks to which it might be exposed with respect to CDR data • adequate procedures and processes to comply with the privacy safeguards including a copy of the policy about the management of CDR data required by privacy safeguard 1 • the applicant's procedures for monitoring, handling, and following up security incidents and security-related customer complaints o the applicant's measures and tools for the prevention of fraud and illegal use of CDR data • descriptions of security control and mitigation measures and procedures for the mandatory reporting of incidents, and notification processes to consumers in the event of a security incident.	• ISMS Policies Specifically a. Data Classification Policy b. Privacy Policy c. Monitoring and Logging Policy d. Incident Management Procedures e. System/Network Security Policy f. Data Destruction Policy g. Risk Management Policy h. Data Breach Policy • Daily Vulnerability Scanning • Data Breach Register
•	The applicant's internal dispute resolution processes meet the requirements specified in the rules and the applicant is a member of an external dispute resolution body recognised by the ACCC (see section 15).	• Internal dispute resolution register
•	The applicant holds appropriate insurance, relevant to the nature and extent of the applicant's management of CDR data.	• Certificate of Currency from insurer

		• Ensure policy terms cover participants

Level and type of Insurance Cover

The insurable events and terms contained within Insurance policies, such as Cyber Insurance policy, are not homogenous. Therefore, without guidance on what types and cover needs to be included, CDR participants are at risk of not being protected by these policies.

We recommend the ACCC engage independent experts to provide advice on this matter.

8. Consent

Summary

- As a general comment, SISS agrees to the proposed rules for consent. However there is no provision for dual or multiple authorisation.
- Where a Consumer provides consent for longer authorisation periods, specific ACCC approved data use cases should be exempt from the 90-day re-authorization process.

8.1.1 Joint Accounts & Complex Authorisations

SISS agrees the authorisation of a joint account where each party has individual authority for CDR can approve the request. However, the proposed model does not support dual or multiple authorisations. If I am a Consumer who has specifically requested this type of authorisation, then it is not in my best interests to have a special exception.

Currently, data can be provided today to Accounting Solution Providers or Data Aggregators, using a model that supports the concepts of dual (or multiple) authorisation.

For example, I am the Owner of a small business employing 15 people. I have an in-house bookkeeper who is authorised to setup things like payments, transfer money, or to fill out the form (or configure within the banking portal) the authorisation of data to go to a TPP. However, the book-keeper is not able to solely approve the authorisation (or may not be able to approve at all). I have a GM and a personal assistant (PA) who, along with myself (the owner), are authorised to approve things the book-keeper does. Any approval requires two of the authorisers to approve. I have specifically requested this to be set up.

In the case of filling out the form to get data, the book-keeper then takes it to any two of the authorisers to get them to sign the form. The form goes off to the ASPSP, and if the signatures are correct, the connection is authorised., until cancelled.

If the approval is via internet banking, then two of the approvers must sign in to authorise the connection.

Under CDR, using the model where the account-request is submitted, then when a user signs into the ASPSP to approve, the normal rules of the ASPSP could be applied. In the case of the example above, the book-keeper would then get two of the authorisers to approve, and request would be completed.

There is one issue that remains, which is created by the time bound reauthorisation. In the above example, after 90 days is up, the book-keeper would have to trigger the reauthorise process and have two of the approvers authorise the data to continue to flow to the TPP.

All account authorization should have access to, and be notified of, any consent provided under CDR.

A history of authorisations for ongoing data connections should be logged and in the event of a data breach be made available o auditors.

In the case of joint accounts or dual authorisation, if reauthorisation is required, the process should be able to be completed by any authoriser, and not restricted to the original authoriser.

8.3.1 Consent should be time limited

SISS does not agree consent should be time limited for **read-only** data sharing where the data use is often on an ongoing basis.

In specific data use cases, the Consumer expects the relationship with the Data Recipient to last over multiple financial years. Asking a Consumer to reauthorise every 90 days is inconvenient, adds risk when other parties providing services to the Consumer could have the data disconnected after 90 days and stifles innovation.

An example of data use that should be exempt from 90-day reauthorising is where data is provided accounting software. Let's assume an accountant is preparing financial accounts and lodging tax forms for a Consumer. If the 90-day period expires, and the Consumer is uncontactable,the data becomes inaccessible and cannot be re-established, as a consequence the accountant will fail to prepare accounts, meet GST and Income tax obligations.

The consumer would not be disadvantaged or put at risk, if the follow CDR functionalities are implemented:

1. Consumer Consent must be sought in order to extend the 90-day reauthorisation period.
2. The Consumer dashboard (permissions) will allow visibility and control for Consumers over their data.

Furthermore, Consumers do not need to reauthorise their mobile banking application on a specified timeframe, which has far more capability than a read-only data feed. So why does a read-only feed require this extra aggravation for a consumer.

As an adjunct to the ACCC registration of a data-recipient, the data-holder also controls access to data by the data-recipient in the following ways:

- A registration by a data-recipient within the data-holder's system to be allowed to collect data.
- A token with permissions to act as consented by the consumer.

Both could be revoked by the data-holder at any time.

- Revoking the data-recipient's registration will prevent them collecting data for all customers who had consented. This is also like what would happen if the data recipient was suspended on the ACCC register.
- Revoking consumer token(s), which would cause any affected consumer to reauthorise.

8.3.2 Consumer Dashboard

Any data-recipient should provide the ability for a Consumer to see what they have consented to, and when the consent was last used. The consumer should be able to revoke consent within the data-recipients solution. A notification of this revocation should also be made to the data-holder, so they can update their solution. If an intermediary is used to obtain data, then this should be clear to the Consumer.

Any data-holder should also provide the same functionality. A consumer should be able to see all the consents active within a data-holders system, should be able to see the last date they were used, and be able to revoke the consent. If the consent has been revoked on the data-holder side, the next call by the data-recipient would mark the consent revoked within the Data Recipient's systems.

With both the above solutions in place, the consumer's ability to direct their data is firmly in their control.

8.3.3 Particular uses noted in the Open Banking Review

Australia could follow a similar system to the UK (ICO) where all data-recipients are required to register as data controllers or data processors and, as part of this, nominate where their data is hosted. This could be recorded within the ACCC data register to allow Consumers to make active choices around where their data is stored.

9. Authorizations & Authentication Process

Summary

- Screen Scraping must be prohibited to give consumers full protection under the CDR an create a level and fair playing field.

We ***do not*** agree with the view expressed in the Final Report of the Review into Open Banking in regard to screen scraping. To allow screen scraping to continue would undermine the security and protection afforded to Data Holders and Data Recipients under the CDR.

We understand the practical implications of a hard-cutoff date being implemented on screen scraping. We recommend a transition period where screen scraping is prohibited from 6 months after a Data Holder makes data available under CDR.

This approach would allow existing screen scraping users to transition across to an approved data supply arrangement with Data Holders and seek consent from their own users.

12. Use of Data

Summary

- Allowing CDR data to be transferred to a non-accredited entity will undermine the data protections for Consumers, and allow by passing of regulation.
- A non-accredited entity should be allowed to access data (with Consumer consent) within an accredited entity, but not be able to transfer data out of that accredited entity's system, unless they themselves become accredited.

In order for consumers to confidently share their data, this trust is built on ensuring all participants are safely and securely managing the Consumer's data.

Therefore, the ACCC position should be that any entity who generates, holds or transmits data as defined by the CDR, must be accredited.

To allow an entity to transmit or store CDR defined data who is not accredited will result in the *by-pass* or *skirting* of the protections the ACCC is seeking to enforce.

If an entity is allowed to use "as directed by the consumer provision" this is a by-pass of their CDR obligations.

It must be noted there is a key distinguishing feature of entities who generate, store & transmit data versus those who are authorised to view (or access) software solutions which contain banking data. A common example would be an Accountant, Financial Planner, guardian or Legal representative (service providers) who may have an authority login into a software solution to perform their role. SISS believes the software solution must be accredited under the CDR requirements, however the service provider does not require accreditation. The software solution has an obligation to protect the consumer's data Practically this would mean an inability for a user to export bank data to a file. Should a service provider wish to store or transmit banking data, then their role has changed and they are now required to meet the CDR accreditation process.

12.1.1 To a Specified entity as directed by the consumer

A Consumer consenting to data being transferred to non-accredited entity ***does not*** make the non-accredited entity systems more secure or reduce the risks for a Data Holder.

It acknowledged that non-accredited entities, such as accountants, require access to the data to perform certain tasks. However, this issue can be easily overcome by the Consumer granting access to non-accredited entity via the Data Recipient system.